A coherent sampling-based method for estimating the jitter used as entropy source for True Random Number Generators

Boyan Valtchanov, Viktor Fischer, Alain Aubert

A coherent sampling-based method for estimating the jitter used as entropy source for True Random Number Generators

Boyan Valtchanov, Viktor Fischer, Alain Aubert

Laboratoire Hubert Curien UMR CNRS 5516, Bât. F 18 Rue du Professeur Benoît Lauras , 42000 Saint Etienne, France.
{boyan.valtchanov,fischer,alain.aubert}@univ-st-etienne.fr

This paper was partially supported by the Rhône-Alpes Region and Saint-Etienne Métropole, France

Abstract:

The paper presents a method, which can be employed to measure the timing jitter present in periodic clock signals that are used as entropy source in true random number generators aimed at cryptographic applications in reconfigurable hardware. The method uses the principle of a coherent sampling and can be easily implemented inside the chip in order to test online the jitter source. The method was carefully validated in various simulations that have shown that the measured jitter size corresponds perfectly to that of the jitter injected to the model. While the primary aim of the proposed measuring technique was the evaluation of the quality of jitter as an entropy source in random number generators, we believe that the same principle can be used in order to characterize the jitter in fast communication links as well.

1. Introduction

In the global communication era, more and more recent industrial applications need to secure data and communications. Many cryptographic primitives and protocols that are used to ensure confidentiality, integrity and authenticity use random number generators in order to generate confidential keys, initial vectors, nonces, padding values, etc. While random bit-stream generators can be easily implemented in analog or mixed-signal devices, the generation of random bit-streams is a challenging task when the generator should be implemented in a logic device like FPGAs (Field-Programmable Gate Arrays). Clearly, logic devices are well suited for algorithmic (pseudo) random number generators, but the true-random number generators need sources of randomness that are difficult to find and explore in logic devices. A mathematical model of the true random number generator (TRNG) is also a crucial element of the cryptographic application design since the final entropy of the generated random bit-stream could be characterized and thus certified if one is able to characterize the physical phenomenon that is used as the entropy source. If the model does not exist, there would be no guarantee that the final entropy of the output stream is true-random, pseudo-random or perhaps a mixture of random and pseudo random phenomena. Characterizing and monitor the entropy source (the jitter) and proposing a mathematical model is the main motivation of the paper.

2. Jitter as an entropy source for TRNGs

Many of the TRNGs known up to date [1], [4], [5], use the jitter present in clock signals (generated using ring oscillators, phase-locked loops or delay-locked loops) as a source of entropy. The quality of the generated random bits is related to the parameters of the clock jitter. In order to avoid jitter manipulations and attacks, it is important to measure these parameters on-line and, if possible, inside the device.

The jitter can be defined as a short-term variation of an event from its ideal position [6]. In general, it is expressed as the variation in time of the zero crossing (rising or falling edge) of the clock signal. The jitter can be a good candidate for randomness generation, since its behavior is closely related to the thermal noise inside semiconductors [2]. The advantage of the thermal noise employed as a source of randomness is that it is relatively difficult to manipulate it in order to realize an attack on the TRNG. The method presented in this paper considers only a true-random (Gaussian) jitter component and it does not take into account the deterministic behavior of the jitter at this stage of our research. For a deeper understanding of the jitter behavior we recommend to read [9].

3. Principle and theoretical background

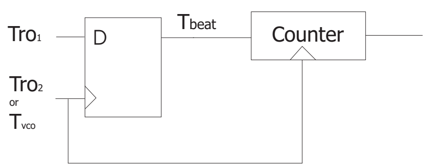

Figure 1: Random jitter component measurement based on the coherent sampling.

The proposed method allows to accurately quantify the random component of the jitter present in clock signals generated inside logic devices. Although the technique can be used to measure the jitter, it has been developed not for measurement or testing purposes, but rather for modeling a TRNG that uses the jitter as a source of randomness.

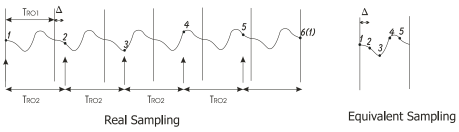

Figure 2: Principle of the coherent sampling.

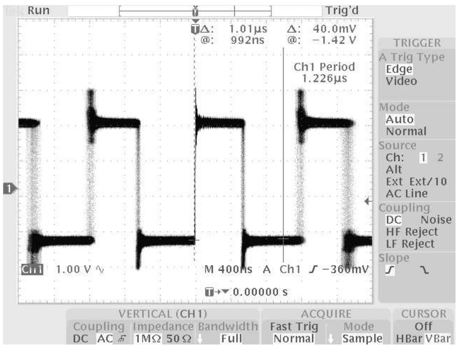

Figure 3: Experimental T_{Beat} signal example.

The proposed measurement technique (see Figure 1) is based on a coherent sampling: the sampling of a periodic signal by another periodic signal featuring similar frequency [3]. The signal on the output of the sampler is called a beat signal and it is a low-frequency signal depending on the frequency difference Δ between the two clock signals T_{ro_1} and T_{ro_2}.

Figure 2 shows the principle of the coherent sampling using two (clock) signals having similar frequencies and the resulting beat signal T_{Beat}, representing the image of T_{ro_1}. An example of this T_{Beat} signal captured on oscilloscope is given in Figure 3. Using the infinite persistence of the oscilloscope, we can clearly see the variations of the period of the beat signal. These variations are the consequence of the jitter present in T_{ro_1} and T_{ro_2} signals. Because of the coherent relationship between the two frequencies, each "half-period" of the beat signal is an integer number of the clock period T_{ro_2}. A counter clocked with this clock signal can thus be used in order to represent these variations. In the next section, we will discuss how we can compute the jitter present in T_{ro_1} by observing the variations in a population of several T_{Beat} periods.

If the proposed technique would be used to measure precisely the jitter of the internal clock signal, one should use an accurate external low phase-noise VCO (Voltage Controlled Oscillator) as a sampling clock and accurately tune its period in relationship to the internal clock period in order to obtain a small Δ. Instead, in order to model the TRNG behavior and to measure the jitter inside the device, we have used two ring oscillators, implemented in the same FPGA. Both oscillators have the same number of inverters. In order to guarantee a small difference between clock periods (Δ), the placement and routing have to be done manually. The final period difference is thus caused mainly by the different delays of the routing scheme selected by the placement and routing tool. Next, we will analyze the case, when only random (Gaussian) jitter component is present in the generated clock signals.

3.1 Measurement of the true-random jitter component

Let us assume that the two clock signals are derived from two internal ring oscillators, and let $T_{ro_{1_{Ideal}}}$ and $T_{ro_{2_{Ideal}}}$ be the two ideal jitter-free periods. We need to achieve a small time period difference between $T_{ro_{1_{Ideal}}}$ and $T_{ro_{2_{Ideal}}}$, namely:

$$T_{ro_{2_{Ideal}}} = T_{ro_{1_{Ideal}}} + \Delta_{Ideal}. \quad (1)$$

This difference comes from the fact that even with the same number of delay elements the two ring oscillators differs due to process variations during manufacturing. With a careful placement, one can obtain Δ of several tens of picoseconds. However the Δ wont be reproducible from one chip to another.
If a random jitter would be included in the previous equations, we obtain:

$$T_{ro_1} = T_{ro_{1_{Ideal}}} + N(0, \sigma_1) = N(T_{ro_{1_{Ideal}}}, \sigma_1) \quad (2)$$

$$T_{ro_2} = T_{ro_{2_{Ideal}}} + N(0, \sigma_2) = N(T_{ro_{2_{Ideal}}}, \sigma_2) \quad (3)$$

Where $N(0, \sigma)$ denote a zero-mean Normal distribution with standard deviation σ.
We can then express the difference Δ by:

$$\Delta = N(T_{ro_{2_{Ideal}}}, \sigma_2) - N(T_{ro_{1_{Ideal}}}, \sigma_1) \quad (4)$$

$$\Delta = N(\Delta_{Ideal}, \sqrt{\sigma_1^2 + \sigma_2^2}) \quad (5)$$

If σ_1 is the same as σ_2, what is the case when the two signals are derived from internal ring oscillators, we get

$$\Delta = N(\Delta_{Ideal}, \sqrt{2}\sigma) \quad (6)$$

Otherwise one should make precise characterization of the VCO used to match the frequencies in order to measure the σ_{VCO}.
According to [8], we can express the length of T_{Beat} as:

$$\frac{T_{Beat}}{\Delta_{Ideal}} = N(\frac{T_{ro_{1_{Ideal}}}}{\Delta_{Ideal}}, \sqrt{\frac{T_{ro_{1_{Ideal}}}}{\Delta_{Ideal}}}\sqrt{\sigma_1^2 + \sigma_2^2}) \quad (7)$$

which, if σ_1 equals σ_2, simplifies to:

$$\frac{T_{Beat}}{\Delta_{Ideal}} = N(\frac{T_{ro_{1_{Ideal}}}}{\Delta}, \sqrt{\frac{T_{ro_{1_{Ideal}}}}{\Delta_{Ideal}}}\sqrt{2}\sigma) \quad (8)$$

The length of the resulting beat signal, T_{Beat} can be then expressed as a normal process:

$$\frac{T_{Beat}}{\Delta_{Ideal}} = N(\mu_{T_{Beat}}, \sigma_{T_{Beat}}) \quad (9)$$

with the mean and standard deviation:

$$\mu_{T_{Beat}} = \frac{T_{ro_{1_{Ideal}}}}{\Delta}, \sigma_{T_{Beat}} = \sqrt{\frac{T_{Ro_{Ideal}}}{\Delta_{Ideal}}}\sqrt{2}\sigma \quad (10)$$

In consequence, if we measure the μ_{T_Beat} and $\sigma_{T_{Beat}}$ using the principle presented in Figure 1, which is based on the use of an 8-bit counter, we can precisely calculate the amount of the random jitter, expressed in 1σ ps, i.e. the RMS jitter (root mean square) present in the two clock signals using equation (11).

$$\sigma = \frac{\sigma_{T_{Beat}} \Delta_{Ideal}}{\sqrt{\frac{T_{Ro_{Ideal}}}{\Delta_{Ideal}}}\sqrt{2}} \tag{11}$$

4. Simulation results

In order to validate equation (11), we have used a simulation model presented in [8] and depicted in Figure 4. The random jitter is generated in text files using Matlab and then injected in VHDL simulation using the Textio package. We have injected different amounts of random jitter (RMS) to the clock signals and analyzed the obtained values of the counter. The $T_{ro_{1_{Ideal}}}$ was set to 5 ns (200Mhz) and Δ to 40 ps. The results of the simulations and recalculated jitter values using equation 11 are presented in Table 4. As it can be seen, the measurement precision that can be achieved is close to 1 ps RMS. Figure 5 present the case for 7 ps RMS jitter present in both T_{ro_1} and T_{ro_2} signals.

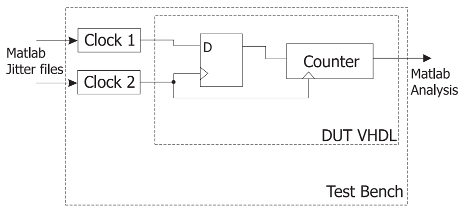

Figure 4: Simulation setup.

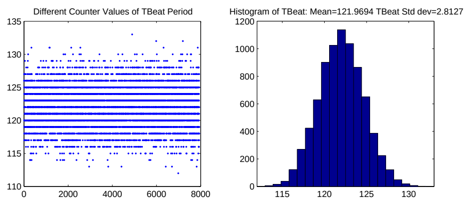

Figure 5: Histogram of the simulated T_{Beat}.

Injected 1σ RMS jitter [ps]	Measured μ_{Tbeat}	Measured σ_{Tbeat}	Calculated 1σ RMS [ps]
10	121.93	4.03	10.19
9	121.98	3.64	9.20
8	121.97	3.24	8.19
7	121.97	2.81	7.10
6	121.98	2.47	6.24

Table 1: Simulation results of the random jitter quantification.

5. Discussion and conclusions

We have proposed a jitter measurement technique that can be embedded in FPGA devices for evaluating and monitoring of the source of randomness employed in true random number generators. The measurement technique can be used as well to characterize the jitter present in high-speed clock signals, if an external VCO (Voltage Controlled Oscillator) is used. The use of an external and precise clock source is necessary in order to closely match the period of the signal under test to the period of the reference clock signal. We have shown by simulation that the measurement error of the proposed method is less than 1 ps RMS of the random component of the jitter.
However, in real world situations and especially inside FPGAs, the jitter can exhibit a non negligible deterministic component due to various factors (power supply variations, cross-talks, R-F interference, etc...). In this case, equation (11) cannot be used for random component jitter quantification and the deterministic jitter has to be considered, too. However, we believe that it is possible to integrate this deterministic behavior of the jitter in the proposed model. This integration is the objective of our current research.

References:

[1] V. Fischer, M. Drutarovsky, M. Simka, and N. Bochard. High performance True Random Number Generator in Altera Stratix FPLDs. *Lecture notes in computer science, FPL'04*, pages 555–564, 2004.

[2] A. Hajimiri and TH Lee. A general theory of phase noise in electrical oscillators. *Solid-State Circuits, IEEE Journal of*, 33(2):179–194, 1998.

[3] J.L. Huang and K.T. Cheng. An On-Chip Short-Time Interval Measurement Technique for Testing High-Speed Communication Links. *Proceedings of the 19th IEEE VLSI Test Symposium*, page 380, 2001.

[4] P. Kohlbrenner and K. Gaj. An embedded true random number generator for FPGAs. *Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays*, pages 71–78.

[5] B. Sunar, W.J. Martin, and D.R. Stinson. A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks. *IEEE TRANSACTIONS ON COMPUTERS*, pages 109–119, 2007.

[6] T. Technologies. Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria. Technical report, GR-253-CORE, 2000.

[7] K.H. Tsoi, K.H. Leung, and P.H.W. Leong. Compact FPGA-based true and pseudo random number generators. *Field-Programmable Custom Computing Machines, 2003. FCCM 2003. 11th Annual IEEE Symposium on*, pages 51–61, 2003.

[8] B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer. Modeling and observing the jitter in ring oscillators implemented in FPGAs. In *Design and Diagnostics of Electronic Circuits and Systems, 2008. DDECS 2008. 11th IEEE Workshop on*, pages 1–6, 2008.

[9] SW Wedge. Predicting random jitter-Exploring the current simulation techniques for predicting the noise in oscillator, clock, and timing circuits. *Circuits and Devices Magazine, IEEE*, 22(6):31–38, 2006.